UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/737,627	12/15/2000	Alastair John Angwin	GB919990123US1	7824

25259 7590 03/09/2005

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/737,627	ANGWIN ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *November 18, 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to request for reconsideration filed on November 18, 2004. No Claims were cancelled. Claim 18 was amended. No new Claims were added. Therefore, presently pending claims are 1 – 26.

2. Typographical errors from the previous office action (May 21, 2004) have been corrected in this office action. For example, includes the original dependent Claim 26 in the explicit statutory rejection. For the basis of rejection of Claim 26, please refer to this and previous office action.

3. This office action also corrects another typographical error for the Claims 1, 7, 12, 18 and 24 from the previous office action (May 21, 2004). "Trieger does not explicitly disclose exchanging a seed value ..." should be read, as "Trieger does not explicitly disclose exchanging a new seed value ...".

Response to Arguments

4. Applicant's arguments filed on November 18, 2004, have been fully considered but they are not persuasive for the following reasons:

5. Applicant argued that the cited prior arts (CPA) [Trieger (U.S. Patent number 6,226,750, hereafter "Trieger") and Anderson (U.S. Patent Number 5,751812, hereafter "Anderson")] do not teach, suggest or disclose exchanging "a seed value, a mathematical advance function or a one-way function", "generating the session-identifying key", "user authentication" and "generating of new seed values for successive attempts to re-initialize communication". Applicant further argues that neither Trieger nor Anderson teaches "exchanging a seed value, a mathematical function and then the subsequent use of the mathematical advance function to change the seed value".

6. Applicant agrees that Anderson teaches client and server exchanging seed value and password.

7. Trieger discloses a method for securely tracking communication in client-server environment comprising the steps of establishing a first connection between a client and a server, authenticating the client at the server, sending a first key (identifier or seed) to the client from the server, generating a request and sending a first key (identifier or seed) to the server from the client. Server generates and sends a new key and a response (number or a flag) to the client (Column 7 line 48 – Column 8 30 and Column 10 lines 42 – 56).

8. Anderson discloses a method for communicating by authenticating the client using a seed, function and generating a hash function (Column 1 line 60 – Column 2 line 14). Anderson further discloses re-initialization function which may be implemented by generating new seed and applying a function to generate a key to transmit to the server from the client (Anderson Column 3 lines 40 - 56).

9. Regarding Claims 1, 7, 12, 18 and 24, Trieger teaches and describes a method for controlling a plurality of separate electronic communications between first and second parties. The method is described with several detailed illustrative (different) embodiments (Trieger Fig.1, 3, 4 and Column 6 line 30 – Column 10 line 26), including the steps of

initially securely exchanging a seed (identifier or key) value between said first and second parties (Trieger Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56), Trieger discloses that the client sends an identifier or key and that the server sends a key (seed) to the client and key is a number of a desired length (See instant application specification on page 3 paragraph [0035] for the description of a seed value);

exchanging a mathematical advance function between said parties (Trieger Column 11 liens 44 – 66 and Column 12 lines 18 – 47), Trieger discloses that the client sends a response (which is used to create a key on the server side) and the server sends a response (which is used to create a key on the client key); and

exchanging a one-way hash function between said parties (Trieger Column 10 lines 42 – 56), Trieger discloses generating a random key (hashing) using an identifier or key to store in the database;

10. Even though Trieger secure communication between the first and second parties by exchanging a seed value, a mathematical advance function and a one-way hash function wherein the process is repeated for any subsequent connections, Trieger does not explicitly discloses exchanging a new seed value prior to each separate communication.

11. However, Anderson discloses a method and apparatus for performing secure re-initialization wherein prior to each separate communication,

applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33), Anderson discloses internally applying advanced function (generating re-initialization by selecting a new seed value and using any number of functions, including addition); (See instant application specification on page 3 paragraph [0031 and 0038] for the description of a mathematical function);

applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33), Anderson discloses applying a hash function to the new seed value;

communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33), Anderson discloses that the encrypted value (code) is transmitted;

comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44), Anderson discloses that the server challenges the client to provide an encrypted value (password or code); and

if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50), Anderson discloses that server notifies the client of the validity of the encrypted code and takes appropriate action to either grant or deny access to the user.

12. Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party with automatic re-initialization, to exchange a new seed value, a mathematical advance function and one-way hash function and the generating and comparing security codes to permit the respective communication to take place as taught by Anderson to provide a secure and multiple communications with a server and client as taught by Trieger.

13. Motivation to combine the teachings of Anderson with Trieger teachings comes from the need to provide improved secure systems in terms of re-initialization security and convenience. Trieger provides a discussion of the need for subsequent

communications to include exchanging a seed value but silent on the specifics of exchanging a new seed value and it would be obvious to one of ordinary skill in the art to combine Trieger with Anderson because Anderson provides details of how to exchange a new seed value prior to each communication.

14. Applicant argued that the cited prior arts (CPA) [Trieger (U.S. Patent Number 6,226,750, hereafter "Trieger"), Anderson (U.S. Patent Number 5,751812, hereafter "Anderson") and Owens et al (U.S. Patent Number 6,338,140, hereafter "Owens"] do not teach, suggest or disclose the teachings of independent Claim 18 and can not be combined with Owens.

15. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

16. In this case, Trieger discloses a method for securely tracking communication in client-server environment comprising the steps of establishing a first connection between a client and a server, authenticating the client at the server, sending a first key

(identifier or seed) to the client from the server, generating a request and sending a first key (identifier or seed) to the server from the client. Server generates and sends a new key and a response (number or a flag) to the client (Column 7 line 48 – Column 8 30 and Column 10 lines 42 – 56). Anderson discloses a method for communicating by authenticating the client using a seed, function and generating a hash function (Column 1 line 60 – Column 2 line 14). Anderson further discloses re-initialization function, which may be implemented by generating new seed and applying a function to generate a key to transmit to the server from the client (Anderson Column 3 lines 40 – 56). Owens discloses a method and/or system for validating subscribers which includes a wireless network, an authentication center which authenticates using the seed cryptographic key for first party by verifying the digital signature (Column 11 lines 2 – 48).

17. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1, 7, 12, 18 and 24. Dependent claims 2-6, 8-11, 13-17, 19-23, 25 and 26 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this and previous (May 21, 2004) office action. Accordingly, the rejection for the pending Claims 1 – 26 is respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 1- 20, and 24 - 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812).

19. Regarding Claim 1, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said method comprising the steps of:

(a) initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

(b) exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

(c) exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(f) communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(g) comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a new seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

(a) initially securely exchanging a seed value between said first and second parities (Anderson Column 1 line 60 – Column 2 line 5);

(b) exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

(c) exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

(f) communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

(g) comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

20. Regarding Claim 7, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26); wherein said means for controlling includes:

means for initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

means for exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for applying said advance function to the seed value to create a new seed value at each of said parities prior to each separate communication (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

means responsive to said security codes being the same at both parties to permit the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a new seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for initially securely exchanging a seed value between said first and second parties (Anderson Column 1 line 60 – Column 2 line 5);

means for exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

means for exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

means for applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

means for applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

means for communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

means for comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

means for responsive to said security codes being the same at both parties to permit the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

21. Regarding Claim 12, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), comprising the steps of:

(a) initially securely exchanging a seed value between said first and second parities (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

(b) exchanging a mathematical advance function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); and

(c) exchanging a one-way hash function between said parties (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(f) communicating said security code generated at said first party to said second party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

(g) comparing said communicated security code with said security code generated at said second party (Column 8 line 62 – Column 9 line 32); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a new seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

(a) initially securely exchanging a seed value between said first and second parities (Anderson Column 1 line 60 – Column 2 line 5);

(b) exchanging a mathematical advance function between said parties (Anderson Column 1 line 60 – Column 2 line 5); and

(c) exchanging a one-way hash function between said parties (Anderson Column 1 line 60 – Column 2 line 5);

said method further comprising, prior to each separate communication, the step of:

(d) applying said advance function to the seed value to create a new seed value at each of said parities (Anderson Column 6 lines 13 – 33);

(e) applying said hash function to said new seed value to create a said security code at each of said parties (Anderson Column 6 lines 13 – 33);

(f) communicating said security code generated at said first party to said second party (Anderson Column 6 lines 13 – 33);

(g) comparing said communicated security code with said security code generated at said second party (Anderson Column 6 lines 13 – 44); and

(h) if said security codes are the same at both parties, permitting the respective communication to take place between said first and second parties (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught

by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

22. Regarding Claim 18, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said client computer comprising:

means for receiving from said server computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for said hash function to said new seed value to create a security code (Column 11 lines 44 – 66 and Column 12 lines 18 – 47); and

means for communicating said security code to said server computer (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

whereby said server computer permits secure communication with said client computer is security code correspondingly calculated by said server is identical to said security codes communicated by said client computer (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a new seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for receiving from said server computer a seed value, a mathematical advance function and a one-way hash function (Anderson Column 1 line 60 – Column 2 line 5);

means for said hash function to said new seed value to create a security code (Anderson Column 6 lines 13 – 33); and

means for communicating said security code to said server computer (Anderson Column 6 lines 13 - 33);

whereby said server computer permits secure communication with said client computer is security code correspondingly calculated by said server is identical to said security codes communicated by said client computer (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

23. Regarding Claim 24, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4

and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56);

means for applying said advance function to said seed value to create a new seed value at each of said parities prior to each separate communication (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for applying said hash function to said new seed value to create a security code (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for receiving a correspondingly calculated security code from said client compute (Column 11 lines 44 – 66 and Column 12 lines 18 – 47);

means for comparing said communicated security codes (Column 8 line 62 – Column 9 line 32); and

means responsive to said security codes being the same to enable secure communication to take place with said client computer (Column 8 line 62 – Column 9 line 60).

Trieger does not explicitly disclose exchanging a new seed value, a mathematical advance function and exchanging a one-way hash function. However, Anderson discloses a method and apparatus for re-initialization function which may be implemented without the need for additional information from the user, the steps comprising:

means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Anderson Column 6 lines 13 - 33);

means for applying said advance function to said seed value to create a new seed value at each of said parities prior to each separate communication (Anderson Column 6 lines 13 - 33);

means for applying said hash function to said new seed value to create a security code (Anderson Column 6 lines 13 - 33);

means for receiving a correspondingly calculated security code from said client compute (Anderson Column 6 lines 13 - 33);

means for comparing said communicated security codes (Anderson Column 6 lines 13 - 44); and

means responsive to said security codes being the same to enable secure communication to take place with said client computer (Anderson Column 6 lines 13 – 50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide automatic re-initialization. The motivation would have been to provide improved secure systems in terms of re-initialization security and convenience.

24. Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Triegar teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said separate communications each follow a disconnection of said first and second parties, said steps (a) to (c) preceding such disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g) (Column 3 lines 38 – 65; Column 8 line 62 – Column 9 line 32; Column 10 lines 42 – 56; Column 11 lines 44 –66; and Column 12 lines 18 – 47).

25. Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

26. Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

27. Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), in which, if said security code is the same, after comparing step (g), comprises further, steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

applying the hash function to said further new seed value to create a further security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

communicating said further security code generated at said second party to said first party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

comparing said further security codes received at said first party with the further security code generated at said first party (Column 8 line 62 – Column 9 line 32 and Anderson Column 6 lines 13 – 44); and

if said further security code is also the same at both nodes, permitting said communication between said first and second parties to take place (Column 8 line 62 – Column 9 line 60 and Anderson Column 6 lines 13 – 50).

28. Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26); wherein said separate communication each follow a disconnection of said first and second parties, said system including means for physically re-establishing said connection between said parties (Column 3 lines 38 – 65).

29. Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

30. Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), including said means for exchanging said advance function and said hash function securely (Anderson Column 6 lines 33).

31. Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said separate communications each follow a disconnection of said first and second parties, said steps (a) to (c) preceding such disconnection, said method including the further step of physically re-establishing said connection between said parties prior to said steps (d) to (g) (Column 3 lines 38 – 65; Column 8 line 62 – Column 9 line 32; Column 10 lines 42 – 56; Column 11 lines 44 –66; and Column 12 lines 18 – 47).

32. Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

33. Claim 16 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication

system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function and said hash function are also exchanged securely (Anderson Column 6 lines 3 – 33).

34. Claim 17 is rejected as applied above in rejecting claim 12. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), in which, if said security code is the same, after comparing step (g), comprises further, steps, prior to permitting resumption of communication between said first and second parties, of:

applying the advance function to said new seed value at each of said parties to create a further new seed value (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

applying the hash function to said further new seed value to create a further security code at each of said parties (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

communicating said further security code generated at said second party to said first party (Column 11 lines 44 – 66 and Column 12 lines 18 – 47; Anderson Column 6 lines 13 – 33);

comparing said further security codes received at said first party with the further security code generated at said first party (Column 8 line 62 and Column 9 line 32; Anderson Column 6 lines 13 – 44); and

if said further security codes are also the same at both parties, permitting said communication between said first and second parties to take place (Column 8 line 62 – Column 9 line 60; Anderson Column 6 lines 13 – 50).

35. Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

36. Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); wherein said advance function is non-recursive (Anderson Column 5 lines 35 – 50).

37. Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Trieger teaches and describes a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

38. Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Trieger teaches and describes a system comprising means of controlling a plurality of separate electronic communications between said first and second parties, by exchange of security codes between said parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26); wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

39. Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Trieger teaches and describes a computer program for use in an electronic communication system for providing communication between at least first party and a second party, said computer program comprising instructions carry out a method of controlling a plurality of separate electronic communications between said first and second parties (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

40. Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

41. Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Trieger teaches and describes a server computer connectable for secure communication with one or more client computers (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26), said server computer comprising means for providing to said client computer a seed value, a mathematical advance function and a one-way hash function (Column 7 line 48 – Column 8 line 30 and Column 10 lines 42 – 56); wherein said advance function is an arithmetic function (Anderson Column 5 lines 35 – 50 and Column 6 lines 13 – 33).

42. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812) further in view of Owens et al. (U.S. Patent No.: 6, 338,140).

43. Claim 21 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does not explicitly disclose a client computer is a cellular telephone (Column 13 lines 45 –

54). However, Owens discloses a method and/or system for validating subscribers which includes a wireless network, an authentication center which authenticates using the seed cryptographic key for first party by verifying the digital signature (Column 11 lines 2 – 48). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to provide wireless cellular telephone to authenticate the user as taught by Ownes. The motivation would have been to provide improved secure systems in cellular telephone.

44. Claim 22 is rejected as applied above in rejecting claim 21. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does not explicitly disclose that a client computer is a WAP enabled (Column 13 lines 44 – 54). However, Owens discloses a method and/or system for validating subscribers which includes a wireless network, an authentication center which authenticates using the seed cryptographic key for first party by verifying the digital signature (Column 11 lines 2 – 48).

45. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Trieger (U.S. Patent No.: 6,226,750) in view of Anderson (U.S. Patent No.: 5,751,812) further in view of Tang (U.S. Patent No.: 6,185,682).

46. Claim 23 is rejected as applied above in rejecting claim 18. Furthermore, Trieger teaches and describes a client computer connectable for secure communication with a server computer (Fig. 1 – 4 and Column 6 line 30 – Column 10 line 26). Trieger does not explicitly disclose a client computer is a personal digital assistant (Column 13 lines 45 – 54). However, Tang discloses an authentication system wherein the client computer is a personal digital assistant (Column 4 lines 2 – 59). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of communication between first party and second party to exchange a seed value, a mathematical advance function and one-way hash function as taught by Anderson and comparing security code with the generated security code to permit the respective communication to take place as taught by Trieger to have a personal digital assistant as client computer as taught by Tang. The motivation would have been to provide improved secure systems in Personal digital assistant.

Conclusion

47. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

48. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
February 24, 2005.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100